PENDING CLAIMS AS AMENDED

Please amend the claims as follows:

1. (Previously presented)   A method used for provisioning an access key to receive broadcast services in a terminal storing a private key comprising:

distributing, over-the-air from the terminal, a public key corresponding to the private key;

receiving, over-the-air at the terminal, a secret key encrypted by the public key;

decrypting the secret key with the private key at the terminal;

receiving the access key at the terminal encrypted by the secret key; and

decrypting the access key at the terminal with the secret key.

2. (Original)   The method of claim 1, wherein the secret key is a registration key.

3. (Original)   The method of claim 1, wherein the secret key is a temporary key.

4. (Previously presented)   The method of claim 1, further comprising:

deriving a short key at the terminal based on the access key;

receiving encrypted broadcast content at the terminal; and

decrypting the encrypted broadcast content at the terminal using the short key.

5. (Previously presented)   A method used for provisioning a broadcast access key to receive broadcast services in a terminal storing a private key comprising:

distributing, over-the-air from the terminal, a public key corresponding to the private key;

receiving, over-the-air at the terminal, the broadcast access key encrypted by the public key; and

decrypting the broadcast access key at the terminal with the private key.

6. (Cancelled)

7. (Cancelled)

8. (Previously presented)   The method of claim 5, further comprising:

      deriving a short key at the terminal based on the broadcast access key;

      receiving encrypted broadcast content at the terminal; and

      decrypting the encrypted broadcast content at the terminal using the short key.

9. (Currently amended)   A method used for provisioning an access key to receive broadcast services in a terminal storing a secret key comprising:

      receiving, over-the-air at the terminal, a public key corresponding to a private key ~~for the terminal~~;

      encrypting the secret key at the terminal with the public key;

      sending, over-the-air from the terminal, the encrypted secret key;

      receiving the access key encrypted by the secret key at the terminal; and

      decrypting the access key ~~by~~ with the secret key at the terminal.

10. (Original) The method of claim 9, wherein the secret key is a registration key.

11. (Original) The method of claim 9, wherein the secret key is a temporary key.

12. (Previously presented)   The method of claim 9, further comprising:

      deriving a short key at the terminal based on the access key;

      receiving encrypted broadcast content at the terminal; and

      decrypting the encrypted broadcast content using the short key at the terminal.

13. (Previously presented)   A method used for distributing an access key to provide broadcast services from a content provider comprising:

      receiving, over-the-air at the content provider, a public key corresponding to a private key;

      encrypting a secret key at the content provider using the public key;

      sending, over-the-air from the content provider, the encrypted secret key;

encrypting the access key using the secret key at the content provider; and

sending the encrypted access key from the content provider.

14. (Original) The method of claim 13, wherein the secret key is a registration key.

15. (Original) The method of claim 13, wherein the secret key is a temporary key.

16. (Previously presented)   A method used for distributing a broadcast access key to provide broadcast services from a content provider comprising:

receiving, over-the-air at the content provider, a public key corresponding to a private key;

encrypting the broadcast access key using the pubic key at the content provider; and

sending, over-the-air from the content provider, the encrypted broadcast access key.

17. (Cancelled)

18. (Cancelled)

19. (Previously presented)   A method used for distributing an access key to provide broadcast services from a content provider having stored a private key comprising:

distributing, over-the-air from the content provider, a public key corresponding to the private key;

receiving, over-the-air at the content provider, a secret key encrypted by the public key;

decrypting the secret key using the private key at the content provider;

encrypting the access key at the content provider using the secret key; and

sending the encrypted access key from the content provider.

20. (Original) The method of claim 19, wherein the secret key is a registration key.

21. (Original) The method of claim 19, wherein the secret key is a temporary key.

22. (Previously presented)   Apparatus for provisioning an access key to receive broadcast services in a terminal storing a private key comprising:

 means for distributing, over-the-air from the terminal, a public key corresponding to the private key;

 means for receiving, over-the-air at the terminal, a secret key encrypted by the public key;

 means for decrypting the secret key with the private key at the terminal;

 means for receiving the access key encrypted by the secret key at the terminal; and

 means for decrypting the access key with the secret key at the terminal.

23. (Original) The apparatus of claim 22, wherein the secret key is a registration key.

24. (Original) The apparatus of claim 22, wherein the secret key is a temporary key.

25. (Previously presented)   Apparatus for provisioning a broadcast access key to receive broadcast services in a terminal storing a private key comprising:

 means for distributing, over-the-air from the terminal, a public key corresponding to the private key;

 means for receiving, over-the-air at the terminal, the broadcast access key encrypted by the public key; and

 means for decrypting the broadcast access key at the terminal with the private key.

26. (Cancelled)

27. (Cancelled)

28. (Previously presented)   Apparatus for provisioning an access key to receive broadcast services in a terminal storing a secret key comprising:

means for receiving, over-the-air at the terminal, a public key corresponding to a private key;

means for encrypting the secret key at the terminal with the public key;

means for sending, over-the-air from the terminal, the encrypted secret key;

means for receiving the access key at the terminal encrypted by the secret key; and

means for decrypting the access key with the secret key.

29. (Original) The apparatus of claim 28, wherein the secret key is a registration key.

30. (Original) The apparatus of claim 28, wherein the secret key is a temporary key.

31. (Previously presented)   Apparatus for distributing an access key to provide broadcast services from a content provider comprising:

means for receiving, over-the-air at the content provider, a public key corresponding to a private key;

means for encrypting a secret key using the public key at the content provider;

means for sending, over-the-air from the content provider, the encrypted secret key;

means for encrypting the access key at the content provider using the secret key; and

means for sending the encrypted access key from the content provider.

32. (Original) The apparatus of claim 31, wherein the secret key is a registration key.

33. (Original) The apparatus of claim 31, wherein the secret key is a temporary key.

34. (Previously presented)   Apparatus for distributing a broadcast access key to provide broadcast services from a content provider comprising:

means for receiving, over-the-air at the content provider, a public key corresponding to a private key;

means for encrypting the broadcast access key at the content provider using the pubic key; and

means for sending, over-the-air from the content provider, the encrypted broadcast access key.

35. (Cancelled)

36. (Cancelled)

37. (Previously presented)   Apparatus for distributing an access key to provide broadcast services from a content provider having stored a private key comprising:

    means for distributing, over-the-air from the content provider, a public key corresponding to the private key;

    means for receiving, over-the-air at the content provider, a secret key encrypted by the public key;

    means for decrypting the secret key at the content provider using the private key;

    means for encrypting the access key at the content provider using the secret key; and

    means for sending the encrypted access key from the content provider.

38. (Original) The apparatus of claim 37, wherein the secret key is a registration key.

39. (Original) The apparatus of claim 37, wherein the secret key is a temporary key.

40. (Previously presented)   Machine readable medium used for provisioning an access key to receive broadcast services in a terminal storing a private key comprising:

    codes for distributing, over-the-air from the terminal, a public key corresponding to the private key;

    codes for receiving, over-the-air at the terminal, a secret key encrypted by the public key;

    codes for decrypting the secret key at the terminal with the private key;

    codes for receiving the access key at the terminal encrypted by the secret key; and

    codes for decrypting the access key at the terminal with the secret key.

41. (Original) The medium of claim 40, wherein the secret key is a registration key.

42. (Original) The medium of claim 40, wherein the secret key is a temporary key.

43. (Previously presented)   Machine readable medium used for provisioning a broadcast access key to receive broadcast services in a terminal storing a private key comprising:

      codes for distributing, over-the-air from the terminal, a public key corresponding to the private key;

      codes for receiving, over-the-air at the terminal, the broadcast access key encrypted by the public key; and

      codes for decrypting the broadcast access key at the terminal with the private key.

44. (Cancelled)

45. (Cancelled)

46. (Previously presented)   Machine readable medium used for provisioning an access key to receive broadcast services in a terminal storing a secret key comprising:

      codes for receiving, over-the-air at the terminal, a public key corresponding to a private key;

      codes for encrypting the secret key at the terminal with the public key;

      codes for sending, over-the-air from the terminal, the encrypted secret key;

      codes for receiving the access key at the terminal encrypted with the secret key; and

      codes for decrypting the access key at the terminal with the secret key.

47. (Original) The medium of claim 46, wherein the secret key is a registration key.

48. (Original) The medium of claim 46, wherein the secret key is a temporary key.

49. (Previously presented)   Machine readable medium used for distributing an access key to provide broadcast services from a content provider comprising:

      codes for receiving, over-the-air at the content provider, a public key corresponding to a private key;

      codes for encrypting a secret key at the content provider using the public key;

      codes for sending, over-the-air from the content provider, the encrypted secret key;

      codes for encrypting the access key at the content provider using the secret key; and

      codes for sending the encrypted access key from the content provider.

50. (Original) The medium of claim 49, wherein the secret key is a registration key.

51. (Original) The medium of claim 49, wherein the secret key is a temporary key.

52. (Previously presented)   Machine readable medium used for distributing a broadcast access key to provide broadcast services from a content provider comprising:

      codes for receiving, over-the-air at the content provider, a public key corresponding to a private key;

      codes for encrypting the broadcast access key at the content provider using the pubic key; and

      codes for sending, over-the-air from the content provider, the encrypted broadcast access key.

53. (Cancelled)

54. (Cancelled)

55. (Previously presented)   Machine readable medium for distributing an access key to provide broadcast services from a content provider having stored a private key comprising:

      codes for distributing, over-the-air from the content provider, a public key corresponding to the private key;

codes for receiving, over-the-air at the content provider, a secret key encrypted by the public key;

    codes for decrypting the secret key at the content provider using the private key;

    codes for encrypting the access key at the content provider using the secret key; and

    codes for sending the encrypted access key from the content provider.

56. (Original) The medium of claim 55, wherein the secret key is a registration key.

57. (Original) The medium of claim 55, wherein the secret key is a temporary key.

58. (Previously presented) A processor used for provisioning an access key to receive broadcast services in a terminal storing a private key, the processor configured to control:

    distributing, over-the-air from the terminal, a public key corresponding to the private key;

    receiving, over-the-air at the terminal, a secret key encrypted by the public key;

    decrypting the secret key from the terminal with the private key;

    receiving the access key at the terminal encrypted by the secret key; and

    decrypting the access key at the terminal with the secret key.

59. (Previously presented) The processor of claim 58, further configured to control:

    deriving a short key based on the access key at the terminal;

    receiving encrypted broadcast content at the terminal; and

    decrypting the encrypted broadcast content at the terminal using the short key.

60. (Previously presented) A processor used for provisioning a broadcast access key to receive broadcast services in a User Identification Module storing a private key, the processor configured to control:

    distributing, over-the-air from the User Identification Module, a public key corresponding to the private key;

    receiving, over-the-air at the User Identification Module, the broadcast access key encrypted by the public key; and

decrypting the broadcast access key at the User Identification Module with the private key.

61. (Previously presented)   The processor of claim 60, further configured to control:

    deriving a short key at the User Identification Module based on the broadcast access key;

    receiving encrypted broadcast content; and

    decrypting the encrypted broadcast content using the short key.

62. (Previously presented)   A processor used for provisioning an access key to receive broadcast services in a terminal storing a secret key, the processor configured to control:

    receiving, over-the-air at the terminal, a public key corresponding to a private key;

    encrypting the secret key at the terminal with the public key;

    sending, over-the-air from the terminal, the encrypted secret key;

    receiving the access key at the terminal encrypted with the secret key; and

    decrypting the access key at the terminal with the secret key.

63. (Previously presented)   The processor of claim 62, further configured to control:

    deriving a short key at the terminal based on the access key;

    receiving encrypted broadcast content; and

    decrypting the encrypted broadcast content using the short key.